AF
JFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): M.J. Coss et al.
Case: 1-1-1
Serial No.: 08/927,382
Filing Date: September 12, 1997
Group: 2131
Examiner: Christopher A. Revak

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: Lisa M. Hanlin Date: July 11, 2005

Title: Methods and Apparatus for a Computer Network Firewall with Multiple Domain Support

---

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith are the following documents relating to the above-identified patent application:

(1) Appeal Brief; and
(2) Copy of Notice of Appeal, filed on April 7, 2005, with copy of stamped return postcard indicating receipt of Notice by PTO on April 11, 2005.

Please extend the period for response by one month to July 11, 2005. Please charge **Ryan, Mason & Lewis, LLP Account No. 50-0762** the amount of $620 ($500 to cover this submission under 37 CFR §1.17(c) and $120 to cover the one month extension fee). In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 50-0762** as required to correct the error. A duplicate copy of this letter is enclosed.

Respectfully submitted,

William E. Lewis

Date: July 11, 2005

William E. Lewis
Reg. No. 39,274
Attorney for Applicant(s)
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): M.J. Coss et al.
Case: 1-1-1
Serial No.: 08/927,382
Filing Date: September 12, 1997
Group: 2131
Examiner: Christopher A. Revak

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature: Lisa M. Hasli Date: July 11, 2005

Title: Methods and Apparatus for a Computer Network Firewall with Multiple Domain Support

---

APPEAL BRIEF

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Applicants (hereinafter referred to as "appellants") hereby appeal the final rejection of claims 1-26 of the above-identified application.

REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc., as evidenced by an assignment recorded March 11, 1998 in the U.S. Patent and Trademark Office at Reel 9036, Frame 0268. The assignee Lucent Technologies Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

An appeal was previously considered by the Board of Patent Appeals and Interferences in the present application. A Decision on Appeal sustaining the prior rejections was issued on January 14, 2004.

STATUS OF CLAIMS

Claims 1-26 stand finally rejected under 35 U.S.C. §102(e) and under 35 U.S.C. §103(a). Claims 1-26 are appealed.

STATUS OF AMENDMENTS

There has been no amendment filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides techniques for implementing a computer network firewall so as to improve processing efficiency, improve security, and increase access rule flexibility (Specification, page 2, lines 12-14). Particularly, in accordance with claimed aspects of the invention, a computer network firewall is able to support: (a) multiple security policies; (b) multiple users; or (c) multiple security policies as well as multiple users, by applying any one of several distinct sets of access rules for a given packet. The particular rule set that is applied for any packet may be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses (Specification, page 2, lines 14-19).

An illustrative embodiment of the claimed invention is shown and explained in the context of FIGs. 5A, 5B, 6 and 7 of the present application. In particular, FIGs. 5A and 5B illustrate a process for a preferred operation of a firewall processor (e.g., firewall processor 111 in FIG. 1 and/or firewall processor 213 in FIG. 2), including the proper selection of a firewall security policy among a plurality of firewall security policies (Specification, page 5, lines 13-14 and 21-22). The security policies can be represented by sets of access rules which may be represented in tabular form (e.g., as is illustrated in one such table in FIG. 3) and which are loaded into the firewall by a firewall administrator (Specification, page 5, lines 23-24).

In a given firewall implementing an illustrative embodiment of the claimed invention, a decision module or engine, called a "domain support engine" (DSE), determines which security policy to use for a new network session. In this illustrative embodiment, each new session must be approved by the security policies of the source domain and the destination domain(s). The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface (Specification, page 9, lines 11-17).

FIGs. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains according to an illustrative embodiment. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required (Specification, page 9, lines 20-23). In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets.

Thus, the claimed invention effectively provides a hierarchical rule selection procedure. That is, before a rule is applied to a particular packet, the appropriate set of rules is first selected, and then a rule from the selected set is applied to the packet.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Whether claims 1-26 are anticipated under 35 U.S.C. §102(e) based on U.S. Patent No. 5,835,726 to Shwed et al. (hereinafter Shwed '726).

II. Whether claims 1-26 are unpatentable under 35 U.S.C. §103(a) based on U.S. Patent No. 5,606,668 to Shwed et al. (hereinafter Shwed '668).

ARGUMENT

Before addressing the grounds of rejection, Appellants provide a short administrative summary of the case.

The present application was filed on September 12, 1997 with claims 1-26. The Examiner rejected claims 1-26 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,606,668 to Shwed. After responses traversing the rejection, Appellants appealed the rejections. In an Appeal Decision dated January 14, 2004, the Board of Patent Appeals and Interferences upheld the rejections.

In view of the Appeal Decision, Appellants filed a Request for Continued Prosecution along with an amendment that amended independent claims 1, 8, 12, 16, 17 and 22. Such an amendment was made in an effort to further clarify the subject matter of the invention and expedite the case through to issuance.

I. Whether claims 1-26 are anticipated under 35 U.S.C. §102(e) based on Shwed '726

Regarding the §102(e) rejection of claims 1-26, Appellants will first reiterate below their remarks presented in their Amendment and Response to Office Action dated September 3, 2004 (Section A) which still apply, followed by remarks addressing the Examiner's latest comments in the outstanding final Office Action (Section B).

A. Remarks Presented in Appellants' Previous Amendment and Response to Office Action

As mentioned above, Appellants previously amended independent claims 1, 8, 12, 16, 17 and 22. More particularly, claims 1, 8, 12, 17 and 22 were amended to recite that a security policy comprises multiple rules. Independent claim 16 was amended to recite that a domain comprises at least one security policy and a security policy comprises multiple rules, and that a plurality of administrators are associated with the plurality of domains.

Appellants amended the claimed invention to further make clear the distinction between a security policy and a rule. That is, a security policy comprises multiple rules. Thus, by way of example, independent claim 1 recites a method for validating a packet in a computer network, comprising the steps of: deriving a session key for said packet; selecting at least one of a plurality of security policies as a function of the session key, wherein a security policy comprises multiple rules; and using the selected at least one of the security policies in validating said packet.

Thus, as is clearly recited, when a packet is received, for example, by a computer implementing the methodology, first a security policy is selected from among a plurality of security policies, then the security policy comprised of its multiple rules is used to validate the packet. Thus, the invention effectively provides a hierarchical rule selection procedure. That is, before a rule is applied to a particular packet, the appropriate security policy is first selected and then, a rule from the selected security policy is applied to the packet.

Shwed '726 does not teach or suggest selecting a security policy having multiple rules from among a plurality of security policies, each having multiple rules.

FIG. 3 of Shwed '726 has been cited in support of the rejection. As column 4, lines 49-50, of Shwed '726 states "FIG. 3 shows the computer screen of the network administrator." Then, column 6, line 62, through column 7, line 11, of Shwed '726 go on to explain:

FIG. 3 shows the computer screen 206 in FIG. 2 in more detail. The screen is broken into four windows, two smaller windows at the left side and two larger windows at the right side. Network objects and services are two aspects of the network which must be defined in the security method of the present invention. Window 304 is used to define network objects such as the workstations, gateways and other computer hardware connected to the system. It is also possible to group various devices together such as, for example, the finance department, the research and development department, the directors of the company. It is thus possible to control data flow not only to individual computers on the network, but also to groups of computers on the network by the appropriate placement of packet filters. This allows the system operator have a great deal of flexibility in the managing of communications on the network. It is possible for example to have the chief financial officer as well as other higher ranking officials of the company such as the CEO and the directors able to communicate directly with the finance group, but filter out communications from other groups. It is also possible to allow electronic mail from all groups but to limit other requests for information to a specified set of computers. This allows the system operator to provide internal as well as external security for the network. The object definition would include the address of the object on the network, as well as a name or group whether the object is internal or external to the network, whether or not a packet filter has been installed on this object and a graphical symbol. The graphical symbol is used in connection with the rule base manager 302.

However, this portion of Shwed '726 merely refers to the fact that a network administrator may specify different security rule sets for different business entities. However, as clearly explained at column 6, lines 42-45, a rule set specified by the network administrator is then processed by the packet filter generator 208 and the resulting code is transmitted to the appropriate packet filter in the network to perform the function that is desired. Then, as explained at column 9, lines 18-50, a packet entering the computer, at a particular connection, on which the packet filter resides is diverted to the packet filter, wherein the associated rule set is applied to validate the packet.

Therefore, unlike the claimed invention, there are no steps in Shwed '726 that, upon receipt of a packet to be validated, first selects a security policy from among a plurality of security policies and then applies the rules associated with that particular policy. Shwed merely applies a rule from the single rule set associated with the packet filter residing on that computer. In fact, Shwed '726 clearly states at column 2, lines 1-4, that a computer merely applies a given security policy to a packet and does not select a security policy from among a plurality of security policies, as in the claimed invention. That is, column 2, lines 1-4, of Shwed '726 states:

> Another object of the invention is to provide a generic packet filter module which is controlled by a set of instructions to implement a given security policy at a node to accept (pass) or reject (drop) the packet wherein the packet is passed only if it passage is preauthorized. (Underlining added for emphasis).

Again, while a network administrator using the Shwed system may take into account different departments and individuals with varying titles at an organization, there is no escaping the fact that a packet filter protecting one or more than one computer is going to apply only the given security policy embodied by the set of instructions programmed into the filter at the packet filter generator. There is no ability disclosed in the Shwed system to have a packet filter receive a packet, then select a security policy from among a plurality of security policies, and then apply the rule set associated with the selected policy. This is what the claimed invention is able to do, but not something that Shwed can do.

Further, regarding independent claim 16, Shwed '726 fails to teach or suggest the elements of claim 16 including a domain comprising at least one security policy and a security policy comprising multiple rules, and that a plurality of administrators are associated with the plurality of domains, wherein multiple rules are administered such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain.

Assuming, *arguendo*, that Shwed discloses multiple administrators, no where does Shwed teach or suggest that, among a plurality of administrators associated with a plurality of domains, only an administrator for a given domain is permitted to modify rules of a security policy for that domain, as in claim 16.

B. Remarks Addressing Examiner's Latest Comments in Final Office Action.

Despite Appellants' sincere attempt to clearly point to the features of claims invention which are clearly distinguishable over Shwed '726 (as reiterated above), the final Office Action fails to address such remarks.

That is, page 2 and 3 of the final Office Action state, in sum, that "a security policy is a collection of rules that dictate how the security policy is to be enforced." This rationale for maintaining the rejections fails to address one of the main arguments previously presented by

Appellants, namely, that there is no ability disclosed in the Shwed system to have a packet filter receive a packet, then select a security policy from among a plurality of security policies, and then apply the rule set associated with the selected policy.

That is, unlike the claimed invention, there are no set of steps taught in Shwed '726 that, upon receipt of a packet to be validated, first selects a security policy from among a plurality of security policies and then applies the rules associated with that particular policy. Shwed merely applies a given security policy to a packet and does not select a security policy from among a plurality of security policies, as in the claimed invention.

Again, while a network administrator using the Shwed system may take into account different departments and individuals with varying titles at an organization, a packet filter protecting one or more than one computer is going to apply only the given security policy embodied by the set of instructions programmed into the filter at the packet filter generator.

So, whether a security policy associated with a packet filter of Shwed represents more than one rule, there is clearly no ability disclosed in the Shwed system to have a packet filter receive a packet, then select a security policy from among a plurality of security policies, and then apply the rule set associated with the selected policy. That is, there is no policy selection followed by rule selection in a packet filter of Shwed.

Thus, Shwed can not disclose "selecting at least one of a plurality of security policies as a function of the session key (data item), wherein a security policy comprises multiple rules, and using the selected at least one of the security policies in validating said packet," as recited in independent claims 1, 17 and 22. Nor can Shwed disclose "designating a plurality of independent security policies, wherein a security policy comprises multiple rules, determining which security policy is appropriate for the packet, and validating the packet using at least a portion of the multiple rules of the determined security policy," as recited in independent claims 8 and 12.

Furthermore, despite the Examiner's contention to the contrary, Shwed does not teach or suggest "segmenting a plurality of security policies into a plurality of domains, wherein a domain comprises at least one security policy and a security policy comprises multiple rules, and further wherein a plurality of administrators are associated with the plurality of domains, and administering

the multiple rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain," as recited in independent claim 16.

Even if one were to agree that Shwed discloses multiple administrators and multiple domains (which Appellants still do not agree with for at least the reasons given above), there is nothing taught nor suggested by Shwed, or argued by the Examiner, that supports "administering the multiple rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain," as recited in independent claim 16.

It is well-established law that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Appellants assert that, for at least the reasons given above in Sections A and B, the rejection based on Shwed '726 does not meet this basic legal requirement. As such, Appellants respectfully assert that independent claims 1, 8, 12, 16, 17 and 22, and the claims which respectively depend therefrom, are patentable over Shwed '726.

II. Whether claims 1-26 are unpatentable under 35 U.S.C. §103(a) based on Shwed '668

Regarding the §103(a) rejection of claims 1-26, Appellants assert that Shwed '668 suffers at least the same deficiencies as Shwed '726. Thus, Appellants reassert and incorporate herein, with respect to this §103(a) rejection of claims 1-26, the arguments presented above with respect to the §102(e) rejection of claims 1-26.

Thus, similar to Shwed '726, Shwed '668 does not teach or suggest selecting a security policy having multiple rules from among a plurality of security policies, each having multiple rules.

The final Office Action cites column 4, lines 23-26, of Shwed '668 in support of the rejection, which states:

> Each of the packet filters operates on a set of instructions which has been generated by the packet filter generator 208 in the system administrator 102. These instructions enable complex operations to be performed on the packet, rather than merely checking the content of the packet against a table containing the parameters for acceptance or rejection of the packet. Thus, each packet filter can handle changes in security rules with great flexibility as well as handle multiple security rules without changing the structure of the packet filter itself.

Shwed '668 (just as in Shwed '726) further states at column 4, line 43, through column 5, line 5:

> FIG. 3 shows the computer screen 206 in FIG. 2 in more detail. The screen is broken into four windows, two smaller windows at the left side and two larger windows at the right side. Network objects and services are two aspects of the network which must be defined in the security method of the present invention. Window 304 is used to define network objects such as the workstations, gateways and other computer hardware connected to the system. It is also possible to group various devices together such as, for example, the finance department, the research and development department, the directors of the company. It is thus possible to control data flow not only to individual computers on the network, but also to groups of computers on the network by the appropriate placement of packet filters. This allows the system operator have a great deal of flexibility in the managing of communications on the network. It is possible for example to have the chief financial officer as well as other higher ranking officials of the company such as the CEO and the directors able to communicate directly with the finance group, but filter out communications from other groups. It is also possible to allow electronic mail from all groups but to limit other requests for information to a specified set of computers. This allows the system operator to provide internal as well as external security for the network. The object definition would include the address of the object on the network, as well as a name or group whether the object is internal or external to the network, whether or not a packet filter has been installed on this object and a graphical symbol. The graphical symbol is used in connection with the rule base manager 302.

Thus again, Shwed merely refers to the fact that a network administrator may specify different security rule sets for different business entities. However, as clearly explained therein, a rule set specified by the network administrator is then processed by the packet filter generator and the resulting code is transmitted to the appropriate packet filter in the network to perform the function that is desired. Then, as explained at column 7, lines 14-47, of Shwed '668, a packet entering the computer, at a particular connection, on which the packet filter resides is diverted to the packet filter, wherein the associated rule set is applied to validate the packet.

Therefore, unlike the claimed invention, there are no steps in Shwed '668 that, upon receipt of a packet to be validated, first selects a security policy from among a plurality of security policies and then applies the rules associated with that particular policy. Shwed merely applies a rule from the single rule set associated with the packet filter residing on that computer. In fact, Shwed '668 also clearly states at column 2, lines 1-4, that a computer merely applies a given security policy to

a packet and does not select a security policy from among a plurality of security policies, as in the claimed invention. That is, column 2, lines 1-4, of Shwed '668 states:

> A still further object of the invention is to provide a generic packet filter module which is controlled by a set of instructions to implement a given security policy at a node to accept (pass) or reject (drop) the packet. (Underlining added for emphasis).

Again, while a network administrator using the Shwed system may take into account different departments and individuals with varying titles at an organization, there is no escaping the fact that a packet filter protecting one or more than one computer is going to apply only the given security policy embodied by the set of instructions programmed into the filter at the packet filter generator. There is no ability disclosed in the Shwed system to have a packet filter receive a packet, then select a security policy from among a plurality of security policies, and then apply the rule set associated with the selected policy. This is what the claimed invention is able to do, but not something that Shwed can do.

Further, regarding independent claim 16, Shwed '668 fails to teach or suggest the elements of claim 16 including a domain comprising at least one security policy and a security policy comprising multiple rules, and that a plurality of administrators are associated with the plurality of domains, wherein multiple rules are administered such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain.

Assuming, *arguendo*, that Shwed discloses multiple administrators, no where does Shwed teach or suggest that, among a plurality of administrators associated with a plurality of domains, only an administrator for a given domain is permitted to modify rules of a security policy for that domain, as in claim 16.

The final Office Action does not address these specific deficiencies, which were first set out in Appellants' previous response dated September 3, 2004.

Furthermore, Appellants assert that the reasons given in the final Office Action for modifying Shwed '668 are deficient, for at least the following reasons.

The Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this

precedent has been reinforced in myriad decisions, and cannot be dispensed with." *In re Lee*, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority." *Id.* at 1343-1344.

In the final Office Action at pages 7-10, the Examiner provides various statement to prove motivation to modify Shwed '668. However, Appellants submit that these statements are based on the type of "subjective belief and unknown authority" that the Federal Circuit has indicated provides insufficient support for an obviousness rejection. More specifically, the Examiner fails to identify any objective evidence of record which supports modification of the single reference.

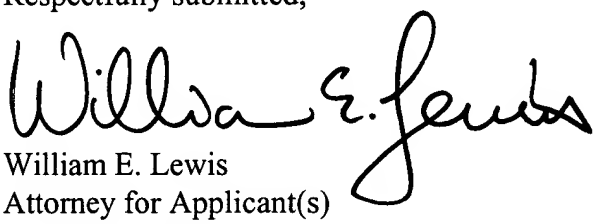
For example, regarding the motivation to modify Shwed '668 to attain the invention of claim 1, the Examiner states at page 7: "processing the extracted packet data in the Shwed invention . . . would be recognized by one of ordinary skill in the art . . . as an obvious equivalent to deriving a session key for the incoming packet, because a session key indicates which security rule to use for the particular packet." However, the Examiner fails to identify any objective evidence of record which would support modification of Shwed '668 to attain this feature.

Further, the final Office Action lumps together a rejection of claims 2, 3, 4, 5, 19, 21, 24 and 26 and states at page 7 that: "it would have been obvious . . . to program the Shwed invention to process all types of Internet packet protocols and to extract all useful packet header data to assist in security rule decision making, because this would be easy to accomplish within the Shwed system and would enable the Shwed system to meet a wide range of user security requirements." Again, the Examiner fails to identify any objective evidence of record which would support modification of Shwed '668 to provide all of the wide ranging features that the Examiner suggests that Shwed could possibly provide.

Similar conclusory statements based on such "subjective belief and unknown authority" are offered at pages 8-10 in support for modifying Shwed to attain the remainder of the claimed features.

For at least the reasons given above, Appellants respectfully assert that independent claims 1, 8, 12, 16, 17 and 22, and the claims which respectively depend therefrom, are patentable over Shwed '668.

Respectfully submitted,



Date: July 11, 2005

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan & Mason, L.L.P.
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946

APPENDIX

1. A method for validating a packet in a computer network, comprising the steps of:

deriving a session key for said packet;

selecting at least one of a plurality of security policies as a function of the session key, wherein a security policy comprises multiple rules; and

using the selected at least one of the security policies in validating said packet.

2. The method of claim 1 wherein the session key includes items derived from header information appended to data in said packet.

3. The method of claim 1 wherein the session key includes at least one item from a set consisting of (i) a source address, (ii) a destination address, (iii) a next-level protocol, (iv) a source port associated with a protocol, and (v) a destination port associated with the protocol.

4. The method of claim 1 wherein the session key includes at least one item from a set consisting of (i) an Internet protocol (IP) source address, (ii) an IP destination address, (iii) a next-level protocol, (iv) the source port associated with the protocol, and (v) the destination port associated with the protocol.

5. The method of claim 3 wherein the next-level protocol is transmission control protocol (TCP) or universal datagram protocol (UDP).

6. The method of claim 1 wherein the network includes a plurality of network interfaces, and wherein the selecting step comprises the step of determining the interface at which the request was received.

7. The method of claim 1 wherein the network includes a plurality of network interfaces, and wherein the selecting step comprises the step of determining the interface to which the request is to be sent.

8. A method for validating a packet in a computer network, comprising the steps of:

designating a plurality of independent security policies, wherein a security policy comprises multiple rules;

determining which security policy is appropriate for the packet; and

validating the packet using at least a portion of the multiple rules of the determined security policy.

9. The method of claim 8 wherein at least a subset of the security policies correspond to different groups associated with a single firewall.

10. The method of claim 8 wherein at least a subset of the security policies correspond to different sub-groups within a given group.

11. The method of claim 8 wherein only an administrator for a given group has access to modify rules of a security policy for that group.

12. An apparatus for use in validating a packet in a firewall of a computer network, the firewall designating a plurality of independent security policies, the apparatus comprising:

a processor associated with the firewall and operative (i) to process the packet to determine which of the security policies is appropriate for the packet, wherein a security policy comprises multiple rules, and (ii) to validate the packet using at least a portion of the multiple rules of the determined security policy.

13. The apparatus of claim 12 wherein at least a subset of the security policies correspond to different groups associated with a single firewall.

14. The apparatus of claim 12 wherein at least a subset of the security policies correspond to different sub-groups within a given group.

15. The apparatus of claim 12 wherein only an administrator for a given group has access to modify rules of a security policy for that group.

16. A method of providing a firewall in a computer network, comprising the steps of:

segmenting a plurality of security policies into a plurality of domains, wherein a domain comprises at least one security policy and a security policy comprises multiple rules, and further wherein a plurality of administrators are associated with the plurality of domains; and

administering the multiple rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain.

17. A computer system for packet validation in a computer network, comprising:

means for obtaining at least one data item from a request for a session;

means for selecting at least one of a plurality of security policies as a function of the data item, wherein a security policy comprises multiple rules; and

means for using the selected at least one of the security policies in validating packets of the session.

18. The computer system of claim 17 wherein the network includes a plurality of network interfaces, and wherein the means for selecting comprises means for determining the interface at which the request was received.

19. The computer system of claim 18 wherein the means for determining comprises means for referring to a source IP address contained in the request.

20. The computer system of claim 17 wherein the network includes a plurality of network interfaces, and wherein the means for selecting comprises means for determining the interface to which the request is to be sent.

21. The computer system of claim 20 wherein the means for determining comprises means for referring to a destination IP address contained in the request.

22. A method for packet validation in a computer network, comprising the steps of:

obtaining at least one data item from a request for a session;

selecting at least one of a plurality of security policies as a function of the data item, wherein a security policy comprises multiple rules; and

using the selected at least one of the security policies in validating packets of the session.

23. The method of claim 22 wherein the network includes a plurality of network interfaces, and the selecting step includes determining the interface at which the request was received.

24. The method of claim 23 wherein the determining step includes referring to a source IP address contained in the request.

25. The method of claim 22 wherein the network includes a plurality of network interfaces, and the selecting step includes determining the interface to which the request is to be sent.

26. The method of claim 25 wherein the determining step includes referring to a destination IP address contained in the request.

PTO/SB/31 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Docket Number (Optional): Coss 1-1-1

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on April 7, 2005

Signature: /Bencivenni/

Typed or printed name: V. Bencivenni

In re Application of: M.J. Coss et al.

Application Number	Filed
08/927,382	September 12, 1997

For: Methods and Apparatus for a Computer Network Firewall with Multiple Domain Support

Art Unit	Examiner
2131	Christopher A. Revak

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 500.00

☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $ _____

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account. I have enclosed a duplicate copy of this sheet.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 50-0762 . I have enclosed a duplicate copy of this sheet.

☑ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☑ attorney or agent of record. Registration number 39,274

☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____

/William E. Lewis/
Signature

William E. Lewis
Typed or printed name

516-759-2946
Telephone number

April 7, 2005
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

Receipt in the USPTO is hereby acknowledged of:

Notice of Appeal - (Orig. & 1 copy)
Petition for Extension of Time Under
37 C.F.R. §1.136(a) - (Orig. & 1 copy)

April 7, 2005
Coss 1-1-1
Serial No. 08/927,382
1200-74